UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/082,758	02/25/2002	Chui-Shan Teresa Lam	09469.014001; 97.0013	5668

22511 7590 04/07/2006

OSHA LIANG L.L.P.
1221 MCKINNEY STREET
SUITE 2800
HOUSTON, TX 77010

EXAMINER	
WINTER, JOHN M	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 04/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/082,758	LAM ET AL.	
	Examiner	Art Unit	
	John M. Winter	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26,30-32,34 and 35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *30-32,34 and 35* is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 1-26,30-32, 34-35 are drawn to retrieving values from a database classified in class 705 subclass 1.

II. Claims 27-29, 33 are drawn to a system for network key management, classified in class 705 subclass 50.

The inventions are distinct, each from the other because of the following reasons:

Inventions I and II are related as combination and subcombination. Inventions in this relationship are distinct if it can be shown that (1) the combination as claimed does not require the particulars of the subcombination as claimed for patentability, and (2) that the subcombination has utility by itself or in other combinations (MPEP § 806.05(c)). In the instant case, the combination as claimed does not require the particulars of the subcombination as claimed such as a hashing module, a serialization module . The subcombinations have separate utility such as hashing a key, and deserializing data (invention II).

Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

Via paper filed on January 30,2006 a provisional election was made without traverse to prosecute the of invention I, claims 6-11. Affirmation of this election must be made by applicant in replying to this Office action. Claims 27-29, 33 are withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Claims 1-26,30-32, 34-35 are pending.

Response to Arguments

The Applicants arguments filed on January 30,2006 have been fully considered.
The amended claims are rejected in view Vaeth et al. (US Patent 6,035,402).
See following rejection

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1- 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over PGP Freeware Users Guide version 7.0 in view of Stein (US Patent 6,370,250) and further in view of Vaeth et al. (US Patent 6,035,402).

As per claim 1,

PGP Freeware discloses a network system for key management, comprising:

a key management system storage providing a secure data storage for the key management system;(Page 45 "placing your public key on a key server")

an application using the key management system to manage an application key;(Figure 4-1)

an interface providing a means for managing the key management system. (Figure 4-1)

wherein the key management comprises a memory storing data within the key management system; a hashing module hashing a key encryption key; an encryption module decrypting data; and a serialization module de-serializing data obtained from the memory, the encryption module, and the serialization module.(Figure 2.2)

PGP Freeware does not explicitly disclose a server; a key management system providing process logic for key management system management located on the server. Stein ('250) discloses a server; a key management system providing process logic for key management system management located on the server; (Figure 1A) It would be obvious to one having ordinary skill in the art at the time the invention was made to combine the PGP Freeware method with the Stein ('250) method in order to persistently store key data.

PGP Freeware does not explicitly disclose wherein the key encryption key comprises a key encryption key PIN, a key encryption key SALT and a key encryption key ITERATION. Vaeth et al. ('402) discloses wherein the key encryption key comprises a key encryption key PIN, a key encryption key SALT and a key encryption key ITERATION; (Column 11, lines 1-26) It would be obvious to one having ordinary skill in the art at the time the invention was made to combine the PGP Freeware method with the Vaeth et al. ('402) method in order to secure key data.

Claim 11 is in parallel with claim 1 and is rejected for at least the same reasons.

As per claim 2,

PGP Freeware discloses the network system of claim 1, further comprising: a client computer operatively connected to the server, wherein the client computer comprises a user interface to manage the key management system. (Pages 48-49 "Getting public keys from a key server")

As per Claim 3
PGP Freeware discloses the network system of claim 1,
wherein the key management storage is located on the server. (Page 45 "placing your public key on a key server")

As per Claim 4
PGP Freeware discloses the network system of claim 1,
wherein the key management storage is located on a second server operatively connected to the server.(Page 45 "placing your public key on a key server")
PGP Freeware discloses the claimed invention except for "a second server ", It would have been obvious to one having ordinary skill in the art at the time the invention was made to use a second server, since it has been held that mere duplication of the essential working parts of a device involves only routine skill in the art. *St Regis Paper Co. v. Bemis Co.*, 193 USPQ 8.

As per Claim 5
PGP Freeware discloses the network system of claim 1,
wherein the interface comprises a graphical user interface. (Figure 4-1)

As per Claim 6
PGP Freeware discloses the network system of claim 5,
Official Notice is taken that "the graphical user interface is integrated into a web browser" is common and well known in prior art in reference to user interfaces. It would have been obvious to one having ordinary skill in the art at the time the invention was made that the user interface would be incorporated into a web browser in order to make the application operating system independent.

As per Claim 7
PGP Freeware discloses the network system of claim 2,
wherein the user interface comprises a graphical user interface.(Figure 4-1)

As per Claim 8
PGP Freeware discloses the network system of claim 7,
Official Notice is taken that "the graphical user interface is integrated into a web browser" is common and well known in prior art in reference to user interfaces. It would have been obvious to one having ordinary skill in the art at the time the invention was made that the user interface would be incorporated into a web browser in order to make the application operating system independent.

As per Claim 9
PGP Freeware discloses the network system of claim 2,
Official Notice is taken that " client computer and the server are connected using an encrypted connection" is common and well known in prior art in reference to networking. It would have been obvious to one having ordinary skill in the art at the time the invention was

made that the client and server would be connected via an encrypted connection in order to prevent malicious theft of data, this is commonly achieved with the SSL protocol.

As per Claim 12
PGP Freeware discloses the network system of claim 1,
further comprising: an encoding module for encoding data. (Figure 2.2)

As per Claim 13
PGP Freeware discloses the network system of claim 10,
wherein the hashing module uses an MD5 hashing function. (Pages 182-183)

As per Claim 14
PGP Freeware discloses the network system of claim 1,
wherein the encryption module further comprises a key generation tool.(Figure 2.2)

As per Claim 15
PGP Freeware discloses the network system of claim 14, wherein the key generation tool comprises a symmetric algorithm. (Pages 182-183)

As per Claim 16
PGP Freeware discloses the network system of claim 14,
wherein the key generation tool comprises an asymmetric algorithm. (Pages 182-183)

As per Claim 17
PGP Freeware discloses the network system of claim 1,
further comprising: an encoding module for encoding data. (Figure 2.2)

As per Claim 18
PGP Freeware discloses the network system of claim 11, wherein the hashing module uses an MD5 hashing function. (Pages 182-183)

As per Claim 19
PGP Freeware discloses the network system of claim 1,
wherein the encryption module further comprises a key generation tool. (Figure 2.2)

As per Claim 20
PGP Freeware discloses the network system of claim 19, wherein the key generation tool comprises a symmetric algorithm. (Pages 182-183)

As per Claim 21
PGP Freeware discloses the network system of claim 19,
wherein the key generation tool comprises an asymmetric algorithm. (Pages 182-183)

As per Claim 22
PGP Freeware discloses the network system of claim 1,
wherein the interface comprises a means for changing a key encryption key.(Page 60 "Examining and setting key properties")

As per Claim 23
PGP Freeware discloses the network system of claim 1,
wherein the interface comprises means for starting the key management system. (Figure 4-1)

As per Claim 24
PGP Freeware discloses the key management system of claim 1,
wherein the interface comprises means for initializing the key management system. (Figure 4-1)

As per Claim 25
PGP Freeware discloses the key management system of claim 1,
wherein the interface comprises means for diagnosing problems with the key management system. (Figure 4-1)

As per Claim 26
PGP Freeware discloses a network system for key management, comprising:
a key management system storage providing a secure data storage for the key management system;(Page 45 "placing your public key on a key server")
an application using the key management system to manage an application key;(Figure 4-1)
an interface providing a means for inputting data into the key management system;(Figure 4-1)
a client computer operatively connected to the server, wherein the client computer comprises a user interface to manage the key management system. (Pages 48-49 "Getting public keys from a key server")
PGP Freeware does not explicitly disclose a server; a key management system providing process logic for key management system initialization located on the server. Stein ('250) discloses a server; a key management system providing process logic for key management system initialization located on the server; (Figure 1A) It would be obvious to one having ordinary skill in the art at the time the invention was made to combine the PGP Freeware method with the Stein ('250) method in order to persistently store key data.
PGP Freeware does not explicitly disclose wherein the key encryption key comprises a key encryption key PIN, a key encryption key SALT and a key encryption key ITERATION. Vaeth et al. ('402) discloses wherein the key encryption key comprises a key encryption key PIN, a key encryption key SALT and a key encryption key ITERATION; (Column 11, lines 1-26) It would be obvious to one having ordinary skill in the art at the time the invention was made to combine the PGP Freeware method with the Vaeth et al. ('402) method in order to secure key data.

Allowable Subject Matter

Claims 30-32, 34-35 are allowable over the prior art record.

Conclusion

Examiners note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Any inquiry of a general nature or relating to the status of this application or concerning this communication or earlier communications from the examiner should be directed to John Winter whose telephone number is **(571) 272-6713**. The Examiner can normally be reached on Monday-Friday, 9:30am-5:00pm. If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, **James Trammell** can be reached at **(571) 272-6712**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://portal.uspto.gov/external/portal/pair . Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to:

(703) 305-7687 [Official communications; including After Final communications labeled "Box AF"]
(703) 308-1396 [Informal/Draft communications, labeled "PROPOSED" or "DRAFT"]

Hand delivered responses should be brought to the Examiner in the Knox Building, 50 Dulany St. Alexandria, VA.

JMW
April 3, 2006

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600